ABSTRACT

A method and apparatus for detecting polymorphic viral code in a computer program is provided. The apparatus comprises an emulator, an operational code analyzer and an heuristic analyzer. The emulator emulates a selected number of instructions of the computer program. The operational code analyzer collects and stores information corresponding to operands and operators used in the instructions and the state of registers/flags after each emulated instruction execution. The heuristic analyzer determines a probability that the computer program contains viral code based on an heuristic analysis of register/flag state information supplied by the operational code analyzer.